## AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Claims 1-11. (Cancelled).

12. (Currently Amended) In a private network comprising a resource and a firewall, which acts as a gateway by controlling client desired access to the private network resource, a method of establishing a connection to the private network resource while balancing authentication processing requirements between a client and the firewall to mutually guard against denial of service attacks, the method comprising steps for:

receiving an assertion from the client that the client has credentials appropriate for accessing the private network resource;

initiating a ~~series~~ plurality of authentication transactions between the client and the firewall, the ~~series~~ plurality of authentication transactions designed to impose commensurable processing burdens on the client requesting access to the private network resource and the firewall operating as a gateway for the private network to mitigate the potential of a client performing a denial of service attack against the private network, wherein the client initially is unaware that the firewall operates as a gateway for the private network, and wherein successful completion of each authentication transaction incrementally increases a level of trust between the client and the firewall;

for each of the ~~series~~ plurality of authentication transactions between the client and the firewall, using a zero-knowledge proof to challenge the client for credentials, the zero-knowledge proof including:

sending a challenge to the client, the correct answer to the challenge obtainable from the asserted credentials without having to arrange the credentials according to a specified layout and without even having to divulge the asserted credentials such that if the client actually possesses the asserted credentials the client can generate the correct answer;

receiving a response from the client including an answer to the challenge, the answer including at least some measure of proof that the client has credentials and that the client's credentials are correct; and

verifying whether or not the answer included in the response the correct answer to the challenge; and

when an acceptable level of probability that the client actually possesses the asserted credentials is reached based on a plurality of correct answers, the firewall granting the client access to the private network resource through the firewall for processing of the asserted credentials.

13. (Cancelled).

14. (Previously Presented) The method of claim 12, wherein the answers are related to at least one of a user's name, client's IP address, password, passport, smart-card or credit card number.

15. (Previously Presented) The method of claim12, wherein a challenge is a question, and wherein one or more client credentials received is an answer to the question.

16. (Original) The method of claim 12, wherein once the client is granted access to the private network resource the only data passed through the firewall from the client are those packets of data destined to the private network resource.

17. (Original) The method of claim 12, wherein the step for granting includes the act of:

establishing an authenticated channel between the firewall and the private network resource, wherein the authenticated channel is established through signing the data from the firewall.

18. (Original) The method of claim 17, further comprising the act of:

discarding any unsigned packets of data received by the private network resource.

19. (Original) The method of claim 12, wherein the private network resource is one of a host, gateway or server.

20. (Original) The method of claim 12, wherein the client is a second firewall.

21. (Original) The method of claim 12, further comprising the act of:

establishing a connection with another resource of a separate private network while simultaneously maintaining a secured channel between the firewall and the client.

22. (Original) The method of claim 12, further comprising the act of:

establishing a connection with another private network resource while simultaneously maintaining a secured channel between the firewall and the client.

23-33. (Cancelled)

34. (Currently Amended) In a private network comprising a resource and a firewall, which acts as a gateway by controlling client desired access to the private network resource, a physical recordable-type computer readable media carrying computer executable instructions that implement a method of establishing a connection to the private network resource while balancing authentication processing requirements between a client and the firewall to mutually guard against denial of service attacks, the method comprising steps for:

receiving an assertion from the client that the client has credentials appropriate for accessing the private network resource;

initiating a ~~series~~ plurality of authentication transactions between the client and the firewall, the ~~series~~ plurality of authentication transactions designed to impose commensurable processing burdens on the client requesting access to the private network resource and the firewall operating as a gateway for the private network to mitigate the potential of a client performing a denial of service attack against the private network, wherein the client initially is unaware that the firewall operates as a gateway for the private network, and wherein successful completion of each authentication transaction incrementally increases a level of trust between the client and the firewall;

for each of the ~~series~~ plurality of authentication transactions between the client and the firewall, using a zero-knowledge proof to challenge the client for credentials, the zero-knowledge proof including:

sending a challenge to the client, the correct answer to the challenge obtainable from the asserted credentials without having to arrange the credentials according to a specified layout and without even having to divulge the asserted credentials such that if the client actually possesses the asserted credentials the client can generate the correct answer;

receiving a response from the client including an answer to the challenge, the answer including at least some measure of proof that the client has credentials and that the client's credentials are correct; and

verifying whether or not the answer included in the response the correct answer to the challenge; and

when an acceptable level of probability that the client actually possess the asserted credentials is reached based on a plurality of correct answers, the firewall granting the client access to the private network resource through the firewall for processing of the credentials.

35. (Cancelled)

36. (Currently Amended) The method of claim 34, wherein the credentials are related to at least one of a user's name, client's IP address, password, passport, smart-card or credit card number.

37. (Previously Presented) The method of claim 34, wherein a challenge is a question, and wherein one or more client credentials received is an answer to the question.

38. (Currently Amended) The method of claim ~~35~~ 34, wherein once the client is granted access to the private network resource the only data passed through the firewall from the client are those packets of data destined to the private network resource.

39. (Original) The method of claim 34, wherein the step for granting includes the act of:

establishing an authenticated channel between the firewall and the private network resource, wherein the authenticated channel is established through signing the data from the firewall.

40. (Original) The method of claim 39, further comprising the act of:

discarding any unsigned packets of data received by the private network resource.

41. (Original) The method of claim 34, wherein the private network resource is one of a host, gateway or server.

42. (Original) The method of claim 34, wherein the client is a second firewall.

43. (Original) The method of claim 34, further comprising the act of:

establishing a connection with another resource of a separate private network while simultaneously maintaining a secured channel between the firewall and the client.

44. (Original) The method of claim 34, further comprising the act of:

establishing a connection with another private network resource while simultaneously maintaining a secured channel between the firewall and the client.

45. (Currently Amended) In a private network comprising a server and a firewall, which acts as a gateway by controlling access to the server, a method of providing access to the server through the firewall without a client knowing about the firewall, the method comprising the acts of:

receiving at the firewall, an access request from the client that is directed to the server because the client does not know that the firewall operates as a gateway for the server;

generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall;

initiating a plurality of authentication transactions between the client and the firewall, the plurality of authentication transactions designed to impose commensurable processing burdens on the client requesting access to the private network resource and the firewall operating as a gateway for the private network to mitigate the potential of a client performing a denial of service attack against the private network, wherein the client initially is unaware that the firewall operates as a gateway for the private network, and wherein successful completion of each authentication transaction incrementally increases a level of trust between the client and the firewall;

for each of the plurality of authentication transactions between the client and the firewall, the firewall using a zero-knowledge proof to challenge the client for credentials, the zero-knowledge proof including:

the firewall sending a request for the client to authenticate to the firewall, the request including the one or more firewall authentication credentials so that the client knows of the level of trust between the server and the firewall without having to make a separate request and further including a challenge, the correct answer to the challenge

obtainable from the asserted credentials without having to arrange the credentials according to a specified layout and without even having to divulge the asserted credentials such that if the client actually possesses the asserted credentials the client can generate the correct answer;

receiving at the firewall, one or more authentication credentials from the client and a response from the client including an answer to the challenge, the answer including at least some measure of proof that the client has credentials and that the client's credentials are correct; and

the firewall verifying the one or more client authentication credentials and whether or not the answer included in the response the correct answer to the challenge; and

thereafter, allowing the client to access the server through the firewall for processing of the authentication credentials.

46. (Original) A method as recited in claim 45, further comprising the acts of:
establishing a secure connection between the firewall and the server; and
forwarding data received from the client to the server over the secure connection.

47. (Original) A method as recited in claim 45, further comprising an acts of:
receiving at the firewall data from the client;
the firewall signing the received data; and
the firewall forwarding the signed data to the server.

48. (Original) A method as recited in claim 45, wherein the server comprises a host or a gateway.

49. (Original) A method as recited in claim 45, wherein the client comprises another firewall.

50. (Original) A method as recited in claim 45, wherein the client maintains a separate connection with another server, and wherein only data intended for the private network passes through the firewall.

51. (Original) A method as recited in claim 50, wherein the other server is part of a separate and distinct virtual private network.

52. (Previously Presented) A method as recited in claim 45, wherein the act of generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall comprises an act of the firewall accessing a private key for the server and using private key to encrypt a portion of data, and further comprising:

an act of including the encrypted portion of data in the request, the encrypted portion of data for use by the client to authenticate the firewall such that the client can use the corresponding public key to decrypt the portion of data and thereby infer that the server trusts the firewall.

53. (Previously Presented) The method as recited in claim 45, wherein the act of generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall comprises an act of generating one or more credentials that permit the firewall to unilaterally authenticate with the client such that the client does not need to have further communications with the firewall to authenticate the firewall.

54. (Currently Amended) The method as recited in claim 12, wherein the step for initiating a ~~series~~ plurality of authentication transactions between the client and the firewall comprises an act of initiating a sequence of exchanges of an interactive proof protocol.

55. (Currently Amended) The method as recited in claim 12, wherein for each of the ~~series~~ plurality of authentication transactions sending a challenge to the client comprises sending a challenge that includes:

a portion of a prior response received from the client; and

a ~~series~~ plurality of random questions, correct answers to the random questions obtainable by the client if the client actually possesses the asserted credentials.

56. (Currently Amended) The method as recited in claim 34, wherein the step for initiating a ~~series~~ plurality of authentication transactions between the client and the firewall comprises an act of initiating a sequence of exchanges of an interactive proof protocol.

57. (Currently Amended) The method as recited in claim 34, wherein for each of the ~~series~~ plurality of authentication transactions sending a challenge to the client comprises sending a challenge that includes:

a portion of a prior response received from the client; and

a ~~series~~ plurality of random questions, correct answers to the random questions obtainable by the client if the client actually possesses the asserted credentials.

58. (Currently Amended) In a private network comprising a server and a firewall, which acts as a gateway by controlling access to the server, a physical recordable-type computer readable media carrying computer executable instructions that implement a method of providing access to the server through the firewall without a client knowing about the firewall, the method comprising the acts of:

receiving at the firewall, an access request from the client that is directed to the server because the client does not know that the firewall operates as a gateway for the server;

generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall;

initiating a plurality of authentication transactions between the client and the firewall, the plurality of authentication transactions designed to impose commensurable processing burdens on the client requesting access to the private network resource and the firewall operating as a gateway for the private network to mitigate the potential of a client performing a denial of service attack against the private network, wherein the client initially is unaware that the firewall operates as a gateway for the private network, and wherein successful completion of each authentication transaction incrementally increases a level of trust between the client and the firewall;

for each of the plurality of authentication transactions between the client and the firewall, the firewall using a zero-knowledge proof to challenge the client for credentials, the zero-knowledge proof including:

the firewall sending a request for the client to authenticate to the firewall, the request including the one or more firewall authentication credentials so that the client knows of the level of trust between the server and the firewall without having to make a separate request and further including a challenge, the correct answer to the challenge obtainable from the asserted credentials without having to arrange the credentials according to a specified layout and without even having to divulge the asserted credentials such that if the client actually possesses the asserted credentials the client can generate the correct answer;

receiving at the firewall, one or more authentication credentials from the client and a response from the client including an answer to the challenge, the answer

including at least some measure of proof that the client has credentials and that the client's credentials are correct; and

the firewall verifying the one or more client authentication credentials and whether or not the answer included in the response the correct answer to the challenge; and

thereafter, allowing the client to access the server through the firewall for processing of the authentication credentials.

59. (Previously Presented) A method as recited in claim 58, wherein the act of generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall comprises an act of the firewall accessing a private key for the server and using private key to encrypt a portion of data, and further comprising:

an act of including the encrypted portion of data in the request, the encrypted portion of data for use by the client to authenticate the firewall such that the client can use the corresponding public key to decrypt the portion of data and thereby infer that the server trusts the firewall.

60. (Previously Presented) The method as recited in claim 58, wherein the act of generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall comprises an act of generating one or more credentials that permit the firewall to unilaterally authenticate with the client such that the client does not need to have further communications with the firewall to authenticate the firewall.